Message

From: Jason Woloz [redacted]@google.com]
Sent: 8/11/2018 9:05:40 PM
To: Bill Bilodeau [redacted]@google.com]
CC: Purnima Kochikar [redacted]@google.com]; Sagar Kamdar [redacted]@google.com]; Jamie Rosenberg [redacted]@google.com]; Sameer Samat [redacted]@google.com]; Dave Kleidermacher [redacted]@google.com]; Tian Lim [redacted]@google.com]; Paul Bankhead [redacted]@google.com]; TI Chang [redacted]@google.com]
Subject: Re: Request for Fortnite Signing Keys

Thanks Bill. I've passed to these on to MUWs to update the bug and whitelist. I'll follow up with you directly if I have further Qs.

On Sat, Aug 11, 2018, 9:38 AM Bill Bilodeau <[redacted]@google.com> wrote:
Here's the reply from Epic:

The SHA1 for Fortnite client is:

SHA1: 9F:09:41:6D:C4:17:59:9E:63:81:04:22:11:B7:96:40:1F:E2:16:98

The SHA1 for Fortnite Installer is:

SHA1: 70:75:66:F8:B0:9B:4C:8B:FD:77:2E:1B:53:6D:58:1F:19:BC:30:12

These are the old two keys which should be considered valid at this time.

On Fri, Aug 10, 2018, 11:32 PM Bill Bilodeau [redacted]@google.com> wrote:
+TI in case I'm not available.

On Fri, Aug 10, 2018, 11:22 PM Bill Bilodeau [redacted]@google.com> wrote:
I'll try sending a message to my contacts at Epic.

Bill

On Fri, Aug 10, 2018, 7:23 PM Purnima Kochikar [redacted]@google.com> wrote:
+Bill Bilodeau

Would you please help here?
P

On Fri, Aug 10, 2018, 17:22 Sagar Kamdar <[redacted]@google.com> wrote:
+Jamie Rosenberg +Purnima Kochikar +Sameer Samat

On Fri, Aug 10, 2018 at 5:20 PM Jason Woloz <[redacted]@google.com> wrote:
Hey Folks,

Who is currently communicating with Fornite and can they help confirm the cert hashes for us so we can ensure we are only flagging counterfeits?

---------- Forwarded message ---------
From: **Trong-Thi, Mai** [redacted]@google.com>
Date: Thu, Aug 9, 2018 at 8:13 PM
Subject: Request for Fortnite Signing Keys

EXHIBIT 1172

To: Jason Woloz <[redacted]@google.com>, Mobile Unwanted Software Core <muws-ops-core@google.com>, Jacob Barrett <[redacted]@google.com>

Hi Jason,

As chatted, we are flagging Fornite impersonating apps and have an automation rule ready to be pushed (https://buganizer.corp.google.com/issues/112342262). The rule contains highly specific signals and we haven't observed any FP.

To avoid flagging the official Fortnite app, we would skip apps signed by Epic's official signing key (aka Certificate - or CERT for short). We have identified 2 official CERTs with SHA1 hash values listed below, but not sure if the list is complete:

"9f09416dc417599e6381042211b796401fe21698"
"707566f8b09b4c8bfd772e1b536d581f19bc3012"

If you have a channel to reach out to Epic, can you check if they are willing to share the SHA1 hashes of the signing keys? This will help us to improve our detection accuracy.

Command to extract CERT information:
```
keytool -list -printcert -jarfile app.apk
```

Thanks,
Thi

---------- Forwarded message ---------
From: Trong-Thi, Mai <[redacted]@google.com>
Date: Fri, Aug 10, 2018 at 12:04 AM
Subject: Re: Whitelisting legit Fortnite everywhere
To: Jason Woloz <[redacted]@google.com>
Cc: Arthur Kaiser <[redacted]@google.com>, Wei Jin <[redacted]@google.com>, Monirul Sharif <[redacted]@google.com>, Chuangang Ren <[redacted]@google.com>, Sebastian Porst <[redacted]@google.com>, [redacted]@google.com>, Sruthi Bandhakavi <[redacted]@google.com>, marmot-eng <[redacted]@google.com>, Google Play Protect Team <[redacted]@google.com>, mUwS Ops <[redacted]@google.com>

Hi Jason,

If Epic can share all their CERT's SHA1/ SHA256 that are different from the ones in Play, we can whitelist apps signed by these CERTs.

On Thu, Aug 9, 2018 at 10:45 PM Jason Woloz <[redacted]@google.com> wrote:
left out the words FP

On Thu, Aug 9, 2018 at 7:42 AM Jason Woloz <[redacted]@google.com> wrote:
Can you send me some details on why its MUWs and evidence. Something I can pass on the folks working with them

On Thu, Aug 9, 2018 at 3:00 AM Trong-Thi, Mai <[redacted]@google.com> wrote:

Quick update: these 3 apps were also classified as MUwS FPs. There could be a chance Epicgames have some debug certs that we don't know about yet. Is it possible for us to reach out?

On Thu, Aug 9, 2018 at 9:44 AM Arthur Kaiser [redacted]@google.com> wrote:
Looks like FTM has already picked up some versions of the real Fortnite game.

Using the cert fingerprint from their dev account, I found 3 versions of the off-market game that are signed with the epic games cert.
(https://plx.corp.google.com/scripts2/script_5b._3922a8_0000_27ce_a8fa_089e082e7164)

Here are the apps:

http://quokka/7dbc36c488f30cdfa62da6246eacbe9d828585096e59f710182eef82e5b0c911

http://quokka/7ffddddc7fac643b465cf532a30fdb91da3476cae9cf9b4bdb4aebfdb9185294

http://quokka/f351dcab47c2f8e8a74be3210003e8a1906ae0c47b83825b39c2eec4a61e8b8b

Going to review these and FP them preemptively so they don't end up in the queue or on an auto-flag list (even though the cert white-list should prevent an auto-flag, just want to be extra cautious here.)

If for some reason they do have PHA attributes I'll start another thread with GPP leads as Sebastian suggested.

Thank you,

Arthur

On Wed, Aug 8, 2018 at 5:17 PM Wei Jin [redacted]@google.com> wrote:
+1 on Monir of having a single place for whitelisting/commenting for general use. I think extending existing comment system to a system that is similar to client side reputation comments makes a lot of sense to me. This can expand our existing Marmot side comment system to a richer syntax (not only used for digest but other entities, such as cert) as we did for reputation comments. It might require some work on how to design a good UI for reviewers to put the comment in and how to show comments in frontend.

Wei

On Wed, Aug 8, 2018 at 5:03 PM Monirul Sharif [redacted]@google.com> wrote:
Thanks Chuangang. Can items in this whitelist be generally used for any Marmot scorer? I mean do you think that the impersonation cert whitelist can be a general whitelist? I was hoping we have a single place for whitelisting for general use.

On Wed, Aug 8, 2018 at 4:54 PM Chuangang Ren [redacted]@google.com> wrote:
For Marmot scoring, we currently have a cert whitelist in Marmot scorer for the purpose of impersonation scorer.

We are now redesigning the cert whitelist this quarter as a OKR. And we can potentially create different cert whitelists for different purposes in scoring phase, i.e., in this case, for safety check.

On Wed, Aug 8, 2018 at 4:31 PM Monirul Sharif [redacted]@google.com> wrote:

Sorry, I guess i didn't clarify properly the scopes. The current reputation comment and cert whitelisting will only apply on server-side/heuristic warnings as Wei mentioned.

To apply something on Marmot-side we'll need a more general commenting system. For the time being, can the Marmot past-review scorer read the reputation comments, Sruthi? That might be a very easy way to extend the whitelisting of reputation to Marmot.

On Wed, Aug 8, 2018 at 4:27 PM Monirul Sharif [redacted]@google.com> wrote:
Just as a general reminder to everyone, please whitelist a cert whenever there is reason to believe we might be generating warnings for those apps.

As part of a comments system, we should possibly think of supporting cert-based comments in Marmot. Adding Yang to include this in his design for the new commenting system that he will soon send out for reviews.

On Wed, Aug 8, 2018 at 3:46 PM Sebastian Porst <[redacted]@google.com> wrote:
Thank you Wei!

On Wed, Aug 8, 2018 at 3:45 PM Wei Jin [redacted]@google.com> wrote:
I whitelisted their cert-fp (sha1: 9f09416dc417599e6381042211b796401fe21698) from any client side reputation system. We also need to find some way of whitelist the cert in Marmot's scan.

Wei

On Wed, Aug 8, 2018 at 2:48 PM Sebastian Porst <[redacted]@google.com> wrote:
Hi teams,

I would appreciate if we could whitelist the official Fortnite before launch. I don't want to get in a situation where any of the automated scorers (or any human really) flags Fortnite accidentally. HR fallout would be severe.

They have an official Google Play account at https://android-cret.corp.google.com/#fusion:id=581524993195&mode=DEV from which you can extract certificate information and other meta-data for whitelisting. Hopefully their final release will have the same signing key and meta-data.

Sebastian
--
You received this message because you are subscribed to the Google Groups "Marmot Engineering" group.
To unsubscribe from this group and stop receiving emails from it, send an email to [redacted]@google.com.
To post to this group, send email to [redacted]@google.com.
To view this discussion on the web visit https://groups.google.com/a/google.com/d/msgid/marmot-eng/CAJiE9EM7eUDFusvmGsG1XY5y6M-BaBXmBdUU%2Bo35TMOrUcAGsw%40mail.gmail.com.
--
You received this message because you are subscribed to the Google Groups "mUwS Ops" group.
To unsubscribe from this group and stop receiving emails from it, send an email to muws-

ops+unsubscribe@google.com.
To post to this group, send email to [redacted]@google.com.
To view this discussion on the web visit https://groups.google.com/a/google.com/d/msgid/muws-ops/CAJiE9ENfCo5vYc9Lc2%2B%3DL62%2BeQ0wzvBx6XMYFckENyQznOBXjw%40mail.gmail.com.

--
You received this message because you are subscribed to the Google Groups "mUwS Ops" group.
To unsubscribe from this group and stop receiving emails from it, send an email to muws-ops+unsubscribe@google.com.
To post to this group, send email to [redacted]@google.com.
To view this discussion on the web visit https://groups.google.com/a/google.com/d/msgid/muws-ops/CAEXvVq8iTXncvAOG%3D7sSn_ic6-aENcMBzZxhLHHHtqtoZt-fjQ%40mail.gmail.com.

--
You received this message because you are subscribed to the Google Groups "Google Play Protect Team" group.
To unsubscribe from this group and stop receiving emails from it, send an email to [redacted]@google.com.
To post to this group, send email to [redacted]@google.com.

--
You received this message because you are subscribed to the Google Groups "mUwS Ops" group.
To unsubscribe from this group and stop receiving emails from it, send an email to muws-[redacted]@google.com.
To post to this group, send email to [redacted]@google.com.
To view this discussion on the web visit https://groups.google.com/a/google.com/d/msgid/muws-ops/CAGRpOT6Y6zyKfRm10YR6DSr4e6G8WeniQNf0OFTrAqM1Q9QpNw%40mail.gmail.com.

--
You received this message because you are subscribed to the Google Groups "mUwS Ops" group.
To unsubscribe from this group and stop receiving emails from it, send an email to [redacted]@google.com.
To post to this group, send email to [redacted]@google.com.
To view this discussion on the web visit https://groups.google.com/a/google.com/d/msgid/muws-ops/CAGfcRk1pUm1sZa4%3D%2BsPKjpkdwZxCSoagxURZC%3DxtvK7pxUq4rQ%40mail.gmail.com.

--
Be well,
Jason

Jason Woloz | Android Security | [redacted]@google.com

--
Be well,
Jason

Jason Woloz | Android Security | [redacted]@google.com

--
Be well,
Jason

Jason Woloz | Android Security | [redacted]@google.com